

Export-Import Bank of the U.S.

§ 403.3

States and its citizens. Accordingly, security classification shall be applied only to protect the national security.

(2) Before a classification determination is made, each item of information that may require protection shall be identified exactly. This requires identification of that specific information, disclosure of which could affect the national security. When there is reasonable doubt about the need to classify, the information should be safeguarded as if it were confidential until a final determination is made by an authorized classifier as to its classification. The final determination must be made within thirty (30) days.

(b) *Classification Designations.* Information which requires protection against unauthorized disclosure in the interest of national security (*classified information*) shall be classified at one of the following three levels:

(1) TOP SECRET shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(2) SECRET shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) CONFIDENTIAL shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

Except as provided by statute, no other terms, such as *SENSITIVE*, *OFFICIAL*, *BUSINESS ONLY*, *AGENCY*, *BUSINESS*, *ADMINISTRATIVELY*, etc., shall be used within the Bank in conjunction with any of the three classification levels defined above.

(c) *Original Classification Authority and Criteria.* (1) The Bank's authority to assign original classification to any document is limited as follows and is nondelegable:

Classification	Classifier
CONFIDENTIAL	President and Chairman. First Vice President and Vice Chairman. General Counsel. Senior Vice Presidents. Security Officer.

(2) A determination to classify information shall be made by an original classification authority when the information concerns one or more of categories (i) through (x) of this paragraph, and when the unauthorized disclosure of the information, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security. Information shall be considered for classification if it concerns:

(i) Military plans, weapons, or operations;

(ii) The vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

(iii) Foreign government information;

(iv) Intelligence activities (including special activities), or intelligence sources or methods;

(v) Foreign relations or foreign activities of the United States;

(vi) Scientific, technological, or economic matters relating to the national security;

(vii) United States Government programs for safeguarding nuclear materials or facilities;

(viii) Cryptology;

(ix) A confidential source; or

(x) Other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President of the United States, by the Chairman or by other officials who have been delegated original classification authority by the President. Recommendations concerning the need to designate additional categories of information that may be considered for classification shall be forwarded through the Security Officer to the Chairman for determination. Such a determination shall be reported to the Director of the Information Security Oversight Office.

(3) Information that is determined to concern one or more of the above categories shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to

§ 403.3

12 CFR Ch. IV (1–12 Edition)

the national security. Accordingly, certain information which would otherwise be unclassified may require classification when associated with other unclassified or classified information. Classification on this basis shall be supported by a written explanation that, at a minimum, shall be maintained with the file or reference on the recent copy of the information.

(4) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or disclosure of intelligence sources or methods is presumed to cause damage to the national security.

(5) Information classified in accordance with the above classification categories shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

(d) *Duration of Original Classification.*

(1) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified. If the date or event for declassification cannot be determined at the time of classification, the standard notation “Originating Agency’s Determination Required”, or its abbreviation “OADR”, should be entered on the “Declassify on” line.

(2) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized declassification authority. These extensions may be by individual documents or categories of information, provided, however, that any extension of classification on other than an individual document basis shall be reported to the Director of the Information Security Oversight Office. The declassification authority shall be responsible for notifying holders of the information of such extensions.

(3) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of the Order.

(e) *Marking and Identification.* (1) Classified information must be marked, or otherwise identified, to inform and warn the holder of the information of its sensitivity. The classifier is responsible for ensuring that proper classification markings are applied. At the time of classification, the following information shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information:

(i) One of the three classification levels defined in § 403.3(b); “(TS)” for Top Secret, “(S)” for Secret, “(C)” for Confidential, and “(U)” for Unclassified; with each page marked at top and bottom according to the highest level of classified information on each page.

(ii) The identity of the original classification authority if other than the person whose name appears as the approving or signing official;

(iii) The agency and office of origin; and

(iv) The date or event for declassification, or the notation “Originating Agency’s Determination Required.”

(2) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. The Chairman may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

(3) Marking designations implementing the provisions of the Order, including abbreviations, shall conform to the standards prescribed in implementing directives issued by the Information Security Oversight Office. All authorized classifiers shall be issued a uniform stamp that has a “Classified by” line and a “Declassify on” line.

(4) Documents that contain foreign government information shall include either the marking, “FOREIGN GOVERNMENT INFORMATION”, or a marking that otherwise indicates that the information is foreign government